DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MEDICAL DEPARTMENT CENTER AND SCHOOL
AND FORT SAM HOUSTON
2250 STANLEY ROAD
FORT SAM HOUSTON, TEXAS 78234-6100

REPLY TO
ATTENTION OF

IMSW-SMH-IM

11 JUL 2006

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Installation Information Management Policy 25-07, Firewalls, Intrusion Detection Systems and Web Filters

1. REFERENCES. References are provided in Appendix A.

2. PURPOSE. To establish an operational firewall, Intrusion Detection System (IDS) and Web filter policy for the Fort Sam Houston (FSH) network environment. This document is in concert with the Defense Information Technology Security Certification and Accreditation Process (DITSCAP) accreditation document.

3. SCOPE. This policy applies to all FSH Local Area Network (LAN), Wide Area Network (WAN), Camp Stanley, Camp Bullis and dial-up connections to and from the FSH network and assigns the responsibility to the Director of Information Management (DOIM) for planning, acquiring, implementing, and maintaining firewalls, IDS sensors and Web filters. The DOIM will provide the technical staff for managing the FSH Network, Firewall, IDS and Web filters. This policy applies to all existing and future firewall, IDS sensors and Web filter implementations for both government and non-government organizations and host based firewall on individual servers and workstations on FSH.

4. POLICY. All connections between the FSH network and equipment outside the Garrison infrastructure shall be routed through the DOIM's installation firewall, IDS sensors and Web filters. Bypassing or defeating the installation firewall, IDS and Web filter systems using modems, leased commercial circuits, Application Service Providers, wireless networking equipment (Wireless Access Points WAP or wireless bridge) or network tunneling software (VPN) to connect directly to outside networks is not permitted.

a. To ensure compliance with this policy, DOIM will:

(1) Determine the need for re-accreditation of FSH network firewall, IDS sensors and webfilter configurations when changes or modifications are necessary and, if needed, will obtain Designated Approving Authority (DAA) approval of the changes.

(2) Ensure only Certified Network or Firewall Administrators perform configuration functions, provide initial and follow-on training for new and changes to existing hardware and software.

(3) Perform Information Assurance Vulnerability Assessments of the effectiveness of the FSH firewall, IDS sensors and webfilter configuration on a periodic basis.

(4) Consider requests for addition, deletion, and changes to Internet Protocol addresses, Domain Name Service, and FSH firewall, IDS sensors and Web filters connectivity.

(5) The Information Assurance Manager (IAM) will inform the DAA of all firewall changes that can cause a change in the acceptable level of risk.

(6) Ensure all firewalls, IDS sensors and Web filters on FSH are operated on dedicated hardware with sufficient capacity to operate in a high-performance environment.

(7) Assess the firewall, IDS sensors and Web filters configuration profile on a periodic basis using FSH approved network security tools and manual procedures.

b. The FSH Firewall Administrators will:

(1) be designated as an Information Assurance Network Officer (IANO).

(2) Comply with applicable DOD and DA guidance/directives and this firewall policy.

(3) Ensure all firewall change requests are documented on a Firewall change request sheet.

(4) Ensure no new services or protocols that allow unrestricted outside connectivity are made operational without prior approval from the FSH DOIM IAM.

(5) Provide future firewall and IDS sensor configuration changes to the DOIM IAM and Information Assurance Network Manager (IANM) for review and approval prior to implementation.

(6) Will submit urgent and routine Access Control Entries (ACE) changes for approval by the IANM.

(7) Perform backups of the firewall and IDS sensors configuration whenever configuration changes are made.

(8) Monitor the firewall and IDS sensors for breaches and attempts to circumvent firewall, IDS sensors or network security.

(9) Report security related incidents to the DOIM IAM and RCERT-TNOSC as required.

(10) Within 30 days after effective date of this policy, provide a report to the DOIM IAM on any existing firewalls, IDS and Web filters. Information will include:

(a) Make and model of the firewall, IDS sensors and Web filters.

(b) Operating system and version.

(c) A copy of the configuration file.

(d) Diagram outlining physical placement of the firewall, IDS sensors and Web filters and its protected network location.

(e) Firewall/IDS administrator(s) POC and telephone number.

(11) The Firewall/IDS/Web filter Administrators will process routine changes within 2-3 workdays from receipt and urgent changes within 1 workday.

c. FSH user and tenants will complete a Firewall Change Request for all network access requirements. (available by contacting DOIM security office at (210) 221-4236 or 221-4760)

5. EXPIRATION. This policy expires 2 years from the implementation date.

6. The point of contact is Mr. Jack D. Poland, Director of Information Management, 221-1300/5281, or email jack.poland1@us.army.mil. The DOIM Information Assurance Manager is Mr. Ralph Coogan, 221-8639, or email address ralph.coogan@us.army.mil.

Encl
Appendix A

RUSSELL J. CZERW
Major General, DC
Commanding

Appendix A

References:

Title 36, Code of Federal Regulations, Chapter 12, "National Archives and Records Administration," Subchapter B, Records Management, July 1, 1999.

DOD Directive 5015.2, Records Management Program, March 6,2000.

DOD Directive 8500.1, Information Assurance, October 24, 2002.

DOD Instruction 8500.2, Information Assurance Implementation, February 6, 2003.

DOD Directive 7740.1, Information Resources Management Program, and all amendments, June 20, 1983.

DOD Directive 7950.1. Automated Data Processing Resources Management, and all amendments, September 29, 1980.

DOD Instruction 5210.74, "Security of DOD Contractor Telecommunications," June 26, 1985.

Public Law 100-235, Computer Security Act, and all amendments, January 8, 1988.

OMB Circular No. A-130, Management of Federal Information Resources and all amendments, February 8, 1996. OMB Circular No. A-130, Revised, Management of Federal Information Resources, November 28, 2000.

National Institute of Standards and Technology, NIST publication 800-7,
http://csrc.nist.gov/publications/nistpubs/800-7/nodel55.html.
Security in Open Systems, July 1994

National Institute of Standards and Technology, NIST publication 800-41, Guidelines on Firewalls and Firewall Policy, 2002.
http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf

NIST94a, NIST. Guideline for the Use of Advanced Authentication Technology Alternatives. Federal Information Processing Standard 190, National Institute of Standards and Technology, September 1994.

NIST94b, NTST. Reducing the Risk of Internet Connection and Use. CSL Bulletin, National Institute of Standard and Technology, May 1994.

DeCA Directive 35-12, "Network Security & Firewall Policy," February 18, 2000.

RFC1244, Paul Holbrook and Joyce Reynolds. RFC 1244: Site Security Handbook, July 1991.

(Continued)

References: (continued)

RFC2196, B. Fraser, Editor. SEI/CMU. RFC 2196: Site Security Handbook. Network Working Group. Multiple contributing authors. September 1997.

Carnegie Melon University Software Engineering Institute: CERT Security Improvement Modules, Design the Firewall System, 1999. http://www.cert.org/security-improvement/.

Computer Security Handbook, 3rd Edition, Hutt, A. E., Bosworth, S.; Hoyt, D.B., John Wiley & Sons, Inc. 1995.

International Computer Security Association (ICSA) Guide to Cryptography, Nichols, R. K., McGraw-Hill, 1998.

Defending Your Digital Assets Against Hackers, Crackers, Spies & Thieves, Nichols, R.K.; Ryan, D.J.; Ryan, J.J.C.H., RSA Press/McGraw-Hill, 2000.

Hacking Exposed 5th Edition, McClure, S.; Scambray, J.; Kurtz, G., Osborne/McGraw-Hill, 2005.